

Navigating Threats In Retail

C-Suite Guide to Security

Introduction

Retail faces an increasingly complex security landscape, complicated by growing cyberattack sophistication. While retail seeks to expand their footprint across physical stores, e-Commerce platforms, mobile apps, and interconnected supply chains, bad actors target this expansion for the opportunity it presents: a broader attack surface, ripe for exploit. Retail must balance this expansion while also strengthening their protections - demands often at odds with one another that require pointed security strategies.

Retailers should urgently strengthen identity and access management, secure increasingly interconnected environments, defend against AI-enabled threats and malicious automation, and adopt security strategies like Zero Trust, AI-driven threat detection, and cyber resilience to effectively prevent, detect, and navigate evolving threats. No small task!

To help provide a starting point for evaluating your current security measures, we compiled a quick guide to navigating retail threats in 2026 and combined it with valuable findings from [Verizon's 2026 Data Breach Investigations Report](#) - the latest edition of their annual deep dive into the state of cybersecurity, data breaches, security trends and more. This year's edition centered on the theme of "keeping a strong foundation in the face of change" - a focus that lends itself readily to the constant changes seen across retail.

5 considerations for retail

The following provides key recommendations the C-Suite needs to consider when navigating security in the retail space.

1. Build an AI + bot defense strategy

Effective bot management uses behavioral analysis, device signals, and risk scoring to distinguish legitimate shoppers from malicious automation, while minimizing friction for real customers.

Automated attacks are responsible for a growing percentage of fraud impacting retailers. Fastly's own [Threat Insights Report](#) found that 49% of total requests across our network originated from bots, meaning nearly half the internet is bots!

Malicious or unwanted bots

Of the bot requests in our analysis, a whopping 99% were from **unwanted** bots. That means the vast majority of bot traffic across the internet has potentially nefarious intent. These unwanted bots are those that have malicious fingerprints, have deceitful user-agents, that are malicious scanners, and so on. These are bots that are pretending to be real users and that likely have malicious intent. These pose a real threat without a strong bot security strategy.

Wanted bots - crawlers and fetchers

The 2026 DBIR took a deep dive on two categories of ‘wanted’ bots - or those that are performing purportedly non-malicious activities. Despite their seemingly ‘good’ surface intent, the two categories of bots - fetchers and crawlers- still have major implications for security, infrastructure strain and costs. The DBIR found that fetcher traffic has grown significantly, with “roughly 15% of non-malicious bot traffic” in their findings “related to AI bots”.

Managing the added traffic from this category of bots can be challenging, especially when working to determine your business’ specific tolerance for each type of bot - do you want your entire site crawled? Or do you want to limit or monetize the use of your information? How are you tackling increased security concerns?

Industry look at crawler and fetchers

Figure 1 shows combined bot traffic (crawlers and fetchers) in DBIR’s research, with an observed 21% growth in global traffic MoM across all industries. DBIR found that human traffic remained relatively the same, while several industries, retail included, saw large growth.

Retail organizations saw a 48% growth in AI traffic. As retail’s business model depends on direct traffic and engagement, AI scraping and crawling should raise major red flags for retailers in regards to content authority, attribution and the overarching impacts to revenue and bottom line.

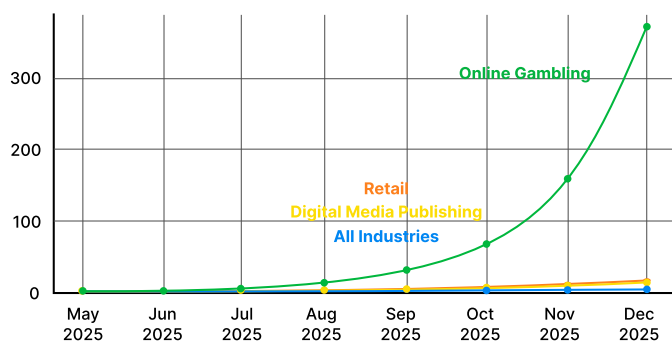


Fig 1. Relative multiplier of Initial Traffic

The Fix

To fully modernize security efforts, retailers should invest in bot management solutions that provide fine-grained control capable of addressing current AI traffic expansion and implications.

At a minimum, orgs must account for an increase in resources (security spend, infrastructure strain, personnel resources, etc). Better still, is an investment in a modern bot management solution.

As AI-generated traffic continues to grow, distinguishing between legitimate automation and malicious bots is increasingly important. Modern bot protection goes beyond simply blocking automated requests - it continuously analyzes behavior, intent, and risk to identify sophisticated threats while allowing trusted users and beneficial AI agents to access your applications. By adapting in real time to evolving attack techniques, a modern bot solution helps prevent account takeover, credential stuffing, scraping, and fraud without sacrificing performance or user experience.

The result is stronger security, greater resilience, and the ability to manage AI traffic while keeping your applications and customers protected.

2. Upgrade web application and API security measures

Web applications and APIs power every stage of the shopping experience, from browsing to checkout. With cybercrime growing, attackers (and attacks) becoming more sophisticated and more automated and AI-assisted tooling adding an additional layer of complexity, organizations must reassess existing security measures to ensure they can keep up.

Consumer expectations are also rising; customers expect secure, frictionless experiences with minimal downtime. Regulations like PCI DSS 4.0 demand stronger continuous protection for payment environments and client-side technologies.

The culmination of these demands is a need for organizations to shift from a security strategy focused solely on preventing known vulnerabilities to one that continuously protects applications and APIs while they are running. By prioritizing runtime visibility, adaptive defenses, and edge-based protection, retailers can better defend against rapidly evolving threats without compromising performance or the customer experience.

The 2026 DBIR found that web app security concerns are rising

System intrusion events rose from 53% in 2025 to 61% of reported incidents in 2026. With social engineering (17%) and basic web app attacks (10%) comprising the 2nd and 3rd positions in 2026. These numbers point toward a growing need for security measures to prioritize web application security.

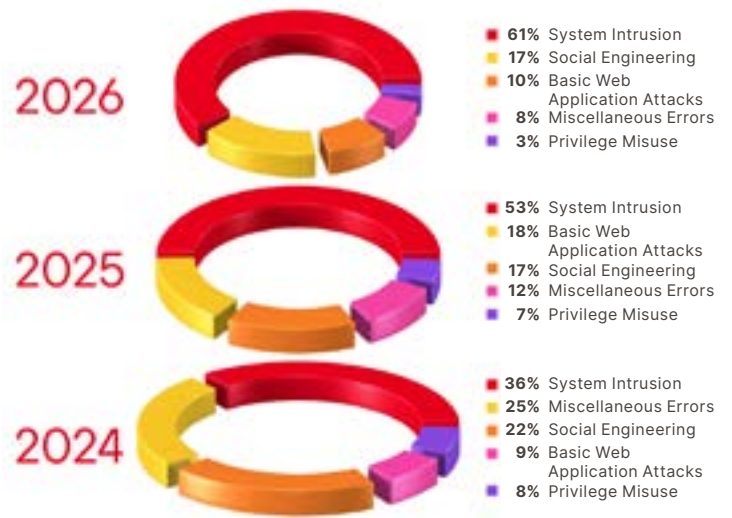


Fig 2. App Security events over time

The Fix

Retailers should evaluate existing security tooling and invest in modern Web Application and API Protection (WAAP), and DDoS solutions, where appropriate. Modern WAFs, API discovery and inventory solutions, API schema validation, and authentication and authorization capabilities should be table stakes.

Prioritizing WAAP helps organizations continuously inspect traffic, detecting malicious behavior, and blocking attacks before they reach applications or origin infrastructure. By combining web application firewalls (WAFs), API security, bot management, and DDoS protection, retailers can reduce risk while maintaining the fast, seamless shopping experiences that customers expect.

Ultimately, strong web application and API protection safeguards both revenue and brand reputation, making it a foundational component of any modern retail security strategy.

3. Secure the customer journey at runtime

Security should extend throughout the live transaction, not just during development. Runtime protections help identify malicious activity as it occurs, including attacks targeting application logic or the customer's browser. This reduces the risk of payment card theft, account compromise, and data exfiltration during active sessions.

The 2026 DBIR noted that “Basic Web Application Attacks remain widespread and are typically driven by stolen credentials and unpatched vulnerabilities. While often low in sophistication, they are highly effective and frequently lead to credential theft, internal data exposure and further compromise of systems”.

They found that 56% of basic web app attacks in 2026 leveraged stolen credentials.

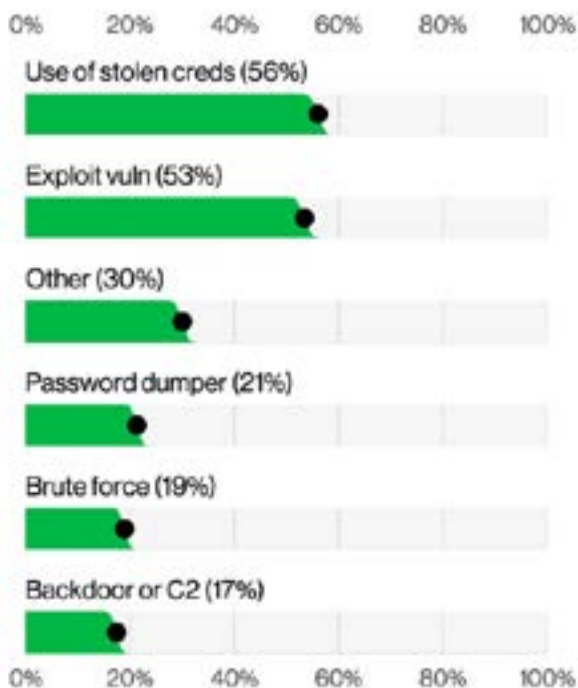


Fig 3. Top Action varieties in Basic Web Application Attacks breaches (n=2,193)

The Fix

Retailers can significantly reduce the risk of stolen credential attacks by combining strong identity protections with intelligent application security. Modern WAAP solutions help detect and block credential stuffing, account takeover attempts, and other automated attacks before they reach login and checkout systems. Adaptive authentication and multi-factor authentication add additional verification when activity appears suspicious. By combining bot protection, behavioral analysis, and risk-based access controls, retailers can protect customer accounts from compromise without creating unnecessary friction for legitimate shoppers.

More specifically:

- **Bot management** can help detect and block automated credential stuffing attacks.
- **WAFs** enable rate limiting which can help restrict repeated login attempts from the same IP, device or account to slow brute-force and credential stuffing attacks.
- **Web App and API protection** combine WAF, bot protection, API security and behavioral analysis to identify and block malicious login attempts.

A modern retail defense strategy should include

- Bot management to stop automated credential stuffing.
- WAAP to secure web applications and APIs.
- Adaptive authentication to verify suspicious login attempts.
- MFA or passkeys to reduce reliance on passwords.
- Behavioral analytics to detect account takeover attempts in real time.

4. Improve visibility and threat detection

As the complexity and scale of cyber threats grows thanks to AI; “LLMs are lowering the barrier to techniques that are less documented and rare - defensive postures will need to catch up”.

Retailers need solutions that give visibility and context to findings. This means comprehensive telemetry across applications, APIs, and edge services enables security teams to detect attacks earlier and respond more effectively. Centralized monitoring and actionable analytics help identify trends, investigate incidents, and continuously refine security controls.

The Fix

An edge cloud platform is a great way to get a consolidated and complete view into your security posture. Improving visibility into threats starts with gaining a complete view of activity across websites, mobile applications, APIs, and customer accounts. By consolidating telemetry from WAFs, bot management, API security, identity systems, and security operations tools into a unified view, retailers can more quickly detect anomalous behavior and prioritize high-risk events. Real-time analytics and behavioral detection provide deeper insight into threats like credential stuffing, account takeover, scraping, and fraud, which allows security teams to respond faster and reduce the impact of attacks before they affect customers or revenue.

5. Deploy Security at the Edge for Performance and Resilience

Modern retail depends on both availability and speed. Deploying security controls at the network edge enables organizations to block malicious traffic, absorb DDoS attacks, enforce access policies, and reduce load on origin infrastructure - all while delivering low-latency experiences to customers.

The DBIR notes that “DDoS attacks continue to be one of the top incidents targeting a wide variety of different industries.”

For retailers, a DDoS attack can have immediate business consequences - from lost revenue and abandoned shopping carts to damaged customer trust and brand reputation. Attackers often target high-traffic events and peak shopping periods, overwhelming websites, APIs, or checkout services to disrupt the customer experience.

In some cases, DDoS attacks are also used to distract security teams while other malicious activity, like credential stuffing or account takeover, takes place. Effective DDoS protection helps ensure online storefronts remain fast, available, and resilient when customers need them most.

The Fix

An edge platform with an integrated CDN helps retailers improve both resilience and security by moving critical application delivery and protection closer to users. By distributing traffic across a global network, the edge absorbs traffic spikes, accelerates content delivery, and helps maintain application availability during peak shopping events or DDoS attacks. At the same time, built-in security services - including WAF, bot management, DDoS protection, API protection, and real-time threat detection - inspect and mitigate malicious traffic before it reaches origin infrastructure. The result is a faster, more reliable shopping experience for customers and a stronger security posture that scales with the demands of modern retail.

DBIR: Retail Trends

To add additional context to our recommendations, we dug into the DBIR's retail-specific findings. You can take these findings and layer them into your evaluation of your current security program.

Known, common risks persist

Retail continues to see similar trends, year over year: Given the prevalence of the same risks over time, organizations should use this information to their advantage and put strategies and tooling in place to defend against known, common security risks. Figure 1 shows six years of retail breaches - note how the same three categories persist, with system intrusion increasing dramatically. Verizon notes that attackers are "increasingly targeting third-party systems and internal corporate data", meaning greater impacts when attacks are successful.

Verizon found that the top three initial access vectors for attacks came from exploitation of vulnerabilities (42%), credential abuse (14%), and phishing (9%). This again highlights how important it is to identify, mitigate and resolve known vulnerabilities and attack types.

The persistence and patterns indicates that attackers are having at least some level of success with this attack strategy. Security strategies should respond in kind.

AI risks need special care

Verizon found that while the total number of incidents "rose slightly YoY", the "number of breaches nearly doubled". This means that attacks are becoming more successful - likely thanks to the increasing sophistication, ease and automation made available by AI.

Verizon notes that the "sheer volume of data up for grabs" continues to mark retailers as attractive targets. Retail's data (valuable financial information) attracts bad actors, with the report citing 85% of actor motives as "financial" in nature.

Verizon discusses the growing challenge of handling AI's impacts, noting that "cybersecurity teams are scrambling to automate handling the surge of AI scanning bots, and AI-driven traffic in general." With retail in the "top three of growth of AI traffic" in this year's report, we can learn a lot about the intent of AI bots. Retail depends upon direct traffic to their sites - managing increased traffic stemming from bots (both legitimate and nefarious) challenges existing security strategies.

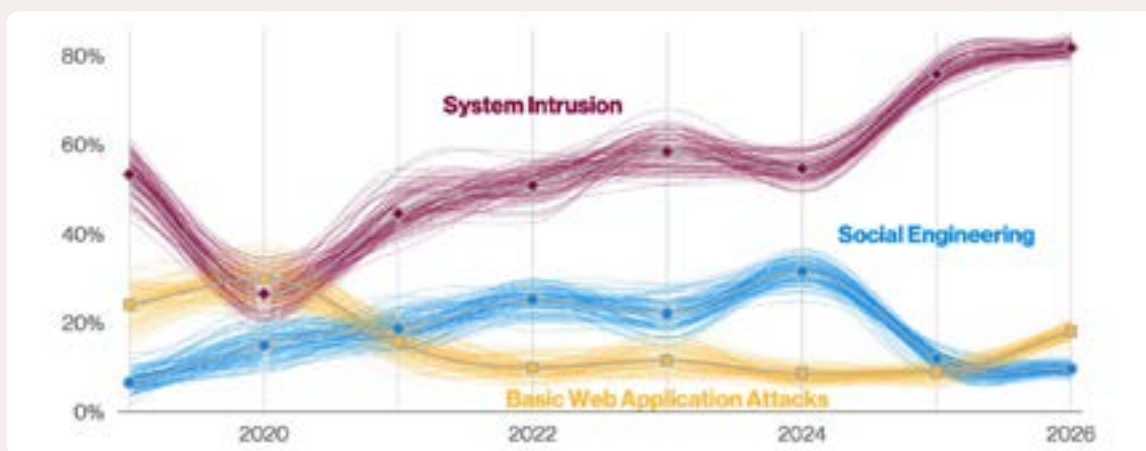


Fig 4. Top patterns in Retail breaches over time (n for 2026 dataset=806)

Everything is a target

Verizon found that “espionage-motivated actors increased again this year, rising from 9% to 19% of breaches where the motive was known”. Espionage here refers to individuals or government-backed groups that steal classified information, trade secrets, technology, or anything of assumed ‘value’.

The growth of this attack type suggests that “more sophisticated actors have taken notice of this sector and are turning their attention to what kinds of useful data their victims may have”. Historically, credit card data was the primary target for bad actors pinpointing retail. Now, attackers are evolving, realizing that they can monetize any data they gather. Internal information like business plans and strategies and internal data and research can all be nabbed for financial gain. This year, Verizon found that internal data is now a target within 84% of attacks, up from 65% last year.

Ransomware is sticky

The 2026 DBIR found that “ransomware remains an ongoing problem across [retail] and was the top malware action in breaches in this sector”. 54% of activities performed during attacks that resulted in data breaches were some form of ransomware.

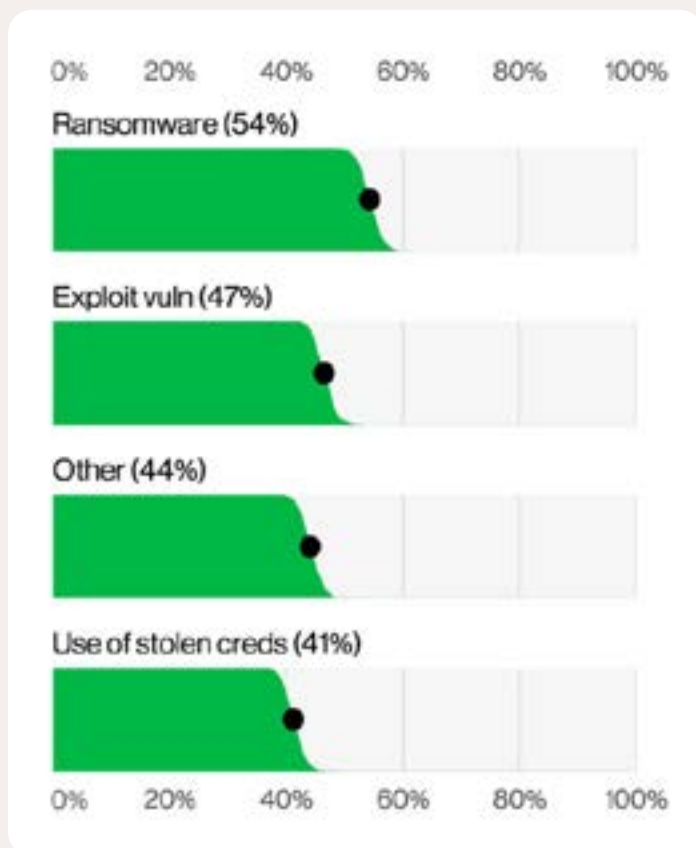


Fig 5. Top Action varieties in Retail breaches (n=719)

Putting it all together: Next Steps

We highly recommend reading the DBIR in its entirety to get a better grasp of global trends and findings.

You can use the recommendations laid out above to assess your existing security strategies and tooling, and begin making improvements and adjustments where necessary.

DBIR was intended to serve as a “baseline” for overall business risk. Verizon advises “When you read about patterns in the data, ask yourself: are we better prepared than this baseline, worse, or about the same? If you’re worse, you know what needs to change. If you’re better, you should be able to point to specific evidence showing why. That’s how you turn industry statistics into actionable risk decisions for your organization”.

For further support, you can read more about Fastly’s AppSec solutions and how they can assist in lowering your retail risk.

Next-Gen WAF

[Fastly’s Next-Gen WAF](#) protects ecommerce applications from common web exploits, including SQL injection, cross-site scripting (XSS), command injection, and other OWASP Top 10 threats. By inspecting requests in real time and adapting to evolving attack techniques, it helps retailers safeguard storefronts, checkout flows, and customer accounts without sacrificing site performance.

Bot Management

[Fastly Bot Management](#) helps retailers distinguish legitimate customers and trusted bots from malicious automation. It detects and mitigates credential stuffing, account takeover attempts, web scraping, inventory hoarding, and other bot-driven attacks, helping protect customer accounts, product availability, and revenue while minimizing friction for real shoppers.

API Security

As retailers increasingly rely on APIs to power mobile apps, checkout, inventory, and customer experiences, [Fastly API Security](#) helps discover, monitor, and protect these critical services. It identifies vulnerable or unmanaged APIs, detects abusive behavior, and blocks attacks before they can disrupt operations or expose sensitive data.

DDoS Protection

[Fastly’s DDoS Protection](#) helps retailers maintain the availability of their websites and applications during traffic floods and application-layer attacks. By absorbing and mitigating malicious traffic at the edge, it keeps storefronts, login services, and checkout experiences available during peak shopping periods and other business-critical events.

Edge Cloud Platform

[Fastly's programmable edge platform](#) enables retailers to deliver secure, personalized digital experiences closer to their customers. Running application logic and security controls at the edge reduces latency, accelerates decision-making, and allows organizations to inspect, filter, and respond to requests before they reach origin infrastructure, strengthening both performance and security.

Observability and Real-Time Logging

Fastly provides [real-time visibility](#) into application traffic and security events, helping retailers detect threats as they emerge. Rich telemetry and integrations with leading SIEM and analytics platforms enable security teams to investigate incidents faster, identify attack patterns, and respond proactively to evolving threats across web applications and APIs.

